

IN THE CLAIMS:

Please amend claims 1, 8, 19, 29-37, 40-43, 47, 49-54, 57, 58, and 61-63, as set forth below.

1 1. (Currently Amended) A computer implemented method comprising:
2 reading distinguished name data from a signed certificate received from a certificate
3 authority; and
4 searching a data structure to identify a certificate signing request associated with the
5 signed certificate, the identified certificate signing request corresponding to the
6 read distinguished name data.

1 2. (Original) The method of claim 1, further comprising identifying a key
2 pair associated with the signed certificate.

1 3. (Original) The method of claim 1, the read distinguished name data
2 comprising all of the distinguished name data contained in the signed certificate.

1 4. (Original) The method of claim 1, the identified certificate signing request
2 corresponding to a portion of the read distinguished name data.

1 5. (Original) The method of claim 1, further comprising importing the
2 signed certificate to a server associated with the identified certificate signing request.

1

1
1 6. (Original) The method of claim 5, wherein the signed certificate is
2 imported to a device that performs SSL processing on behalf of the server.

1
1 7. (Original) The method of claim 1, further comprising identifying at least
2 two certificate signing requests associated with the signed certificate.

1
1 8. (Currently Amended) A computer implemented method comprising:
2 providing a mapping table including distinguished name data for each of a plurality of
3 certificate signing requests;
4 extracting distinguished name data from a signed certificate received from a certificate
5 authority; and
6 comparing the extracted distinguished name data with the mapping table data to identify
7 a certificate signing request associated with the signed certificate from the
8 plurality of certificate signing requests.

1
1 9. (Original) The method of claim 8, the mapping table including at least a
2 common name for each of the plurality of certificate signing requests.

1
1 10. (Original) The method of claim 8, the extracted distinguished name data
2 comprising all of the distinguished name data contained in the signed certificate.

1

1 11. (Original) The method of claim 8, the extracted distinguished name data
2 comprising a common name.

1

1 12. (Original) The method of claim 8, further comprising comparing a portion
2 of the extracted distinguished name data with a portion of the distinguished name data of
3 each certificate signing request contained in the mapping table to identify the certificate
4 signing request associated with the signed certificate.

1

1 13. (Original) The method of claim 12, the portion of the extracted
2 distinguished name data comprising a common name.

1

1 14. (Original) The method of claim 8, further comprising:
2 comparing the extracted distinguished name data with the mapping table data to identify
3 at least two certificate signing requests from the plurality of certificate signing
4 requests; and
5 determining which of the at least two certificate signing requests is associated with the
6 signed certificate.

1

1 15. (Original) The method of claim 14, further comprising performing a
2 second search of the mapping table data to determine which of the at least two certificate
3 signing requests is associated with the signed certificate.

1

1

1 16. (Original) The method of claim 8, further comprising importing the
2 signed certificate to a server associated with the identified certificate signing request.

1

1 17. (Original) The method of claim 16, wherein the signed certificate is
2 imported to a device that performs SSL processing on behalf of the server.

1

1 18. (Original) The method of claim 8, further comprising identifying at least
2 two certificate signing requests associated with the signed certificate.

1

1 19. (Currently Amended) A computer implemented method comprising:
2 generating a certificate signing request, the certificate signing request including
3 distinguished name data;
4 storing the distinguished name data in a mapping table;
5 transmitting the certificate signing request to a certificate authority;
6 receiving a signed certificate from the certificate authority, the signed certificate
7 including distinguished name data;
8 extracting the distinguished name data from the signed certificate; and
9 comparing the extracted distinguished name data with the stored distinguished name data
10 contained in the mapping table to identify the certificate signing request.

1

1 20. (Original) The method of claim 19, the stored distinguished name data
2 comprising all of the distinguished name data contained in the certificate signing request.

1

1

1 21. (Original) The method of claim 19, the stored distinguished name data
2 comprising a common name.

1

1 22. (Original) The method of claim 19, further comprising comparing a
2 portion of the extracted distinguished name data with a portion of the stored distinguished
3 name data.

1

1 23. (Original) The method of claim 19, further comprising comparing a
2 common name contained in the extracted distinguished name data with a common name
3 contained in the stored distinguished name data.

1

1 24. (Original) The method of claim 19, the extracted distinguished name data
2 comprising all of the distinguished name data contained in the signed certificate.

1

1 25. (Original) The method of claim 19, the extracted distinguished name data
2 comprising a common name.

1

1 26. (Original) The method of claim 19, further comprising:
2 generating a key pair associated with the certificate signing request; and
3 identifying the key pair when comparing the extracted distinguished name data with the
4 stored distinguished name data.

1

1
1 27. (Original) The method of claim 19, further comprising importing the
2 signed certificate to a server associated with the certificate signing request.

1
1 28. (Original) The method of claim 19, further comprising importing the
2 signed certificate to an SSL processing device.

1
1 29. (Currently Amended) A computer system comprising:
2 a memory coupled with a bus, the memory having a mapping table resident thereon; and
3 a processing device coupled with the bus, the processing device programmed to perform
4 operations including
5 read reading distinguished name data from a signed certificate received
6 from a certificate authority, and
7 search searching the mapping table to identify a certificate signing request
8 associated with the signed certificate, the identified certificate
9 signing request corresponding to the read distinguished name data.

1
1 30. (Currently Amended) The computer system of claim 29, wherein the
2 processing device is programmed to perform operations further including identify
3 identifying a key pair associated with the signed certificate.

1
1 31. (Currently Amended) The computer system of claim 29, the read
2 distinguished name data comprising all of the distinguished name data contained in the
3 signed certificate.

1
1 32. (Currently Amended) The computer system of claim 29, the identified
2 certificate signing request corresponding to a portion of the read distinguished name data.

1
1 33. (Currently Amended) The computer system of claim 29, the memory
2 comprising a non-volatile data storage device.

1
1 34. (Currently Amended) The computer system of claim 29, wherein a
2 plurality of servers are coupled with the bus, and the processing device is programmed to
3 perform operations further including download downloading the signed certificate to a
4 selected server of the plurality of servers, the selected server associated with the
5 identified certificate signing request.

1
1 35. (Currently Amended) The computer system of claim 29, wherein an SSL
2 processing device is coupled with the bus, and the processing device is programmed to
3 perform operations further including download downloading the signed certificate to the
4 SSL processing device.

1 36. (Currently Amended) An article of manufacture comprising:
2 a ~~machine accessible~~ computer readable medium providing content that, when accessed
3 by a ~~machine~~ computer, causes the ~~machine~~ computer to
4 read distinguished name data from a signed certificate received from a certificate
5 authority; and
6 search a data structure to identify a certificate signing request associated with the
7 signed certificate, the identified certificate signing request corresponding
8 to the read distinguished name data.

1 37. (Currently Amended) The article of manufacture of claim 36, wherein the
2 content, when accessed, further causes the ~~machine~~ computer to identify a key pair
3 associated with the signed certificate.

1 38. (Original) The article of manufacture of claim 36, the read distinguished
2 name data comprising all of the distinguished name data contained in the signed
3 certificate.

1 39. (Original) The article of manufacture of claim 36, the identified certificate
2 signing request corresponding to a portion of the read distinguished name data.

1 40. (Currently Amended) The article of manufacture of claim 36, wherein the
2 content, when accessed, further causes the ~~machine~~ computer to import the signed
3 certificate to a server associated with the identified certificate signing request.

1
1 41. (Currently Amended) The article of manufacture of claim 40, wherein the
2 content, when accessed, further causes the ~~machine~~ computer to import the signed
3 certificate to a device that performs SSL processing on behalf of the server.

1
1 42. (Currently Amended) The article of manufacture of claim 36, wherein the
2 content, when accessed, further causes the ~~machine~~ computer to identify at least two
3 certificate signing requests associated with the signed certificate.

1 43. (Currently Amended) An article of manufacture comprising:
2 a ~~machine accessible~~ computer readable medium providing content that, when accessed
3 by a ~~machine~~ computer, causes the ~~machine~~ computer to
4 provide a mapping table including distinguished name data for each of a plurality
5 of certificate signing requests;
6 extract distinguished name data from a signed certificate received from a
7 certificate authority; and
8 compare the extracted distinguished name data with the mapping table data to
9 identify a certificate signing request associated with the signed certificate
10 from the plurality of certificate signing requests.

1

1 44. (Original) The article of manufacture of claim 43, the mapping table
2 including at least a common name for each of the plurality of certificate signing requests.

1

1 45. (Original) The article of manufacture of claim 43, the extracted
2 distinguished name data comprising all of the distinguished name data contained in the
3 signed certificate.

1

1 46. (Original) The article of manufacture of claim 43, the extracted
2 distinguished name data comprising a common name.

1

1 47. (Currently Amended) The article of manufacture of claim 43, wherein the
2 content, when accessed, further causes the ~~machine~~ computer to compare a portion of the
3 extracted distinguished name data with a portion of the distinguished name data of each
4 certificate signing request contained in the mapping table to identify the certificate
5 signing request associated with the signed certificate.

1

1 48. (Original) The article of manufacture of claim 47, the portion of the
2 extracted distinguished name data comprising a common name.

1

1

1 49. (Currently Amended) The article of manufacture of claim 43, wherein the
2 content, when accessed, further causes the ~~machine~~ computer to:
3 compare the extracted distinguished name data with the mapping table data to identify at
4 least two certificate signing requests from the plurality of certificate signing
5 requests; and
6 determine which of the at least two certificate signing requests is associated with the
7 signed certificate.

1

1 50. (Currently Amended) The article of manufacture of claim 49, wherein the
2 content, when accessed, further causes the ~~machine~~ computer to perform a second search
3 of the mapping table data to determine which of the at least two certificate signing
4 requests is associated with the signed certificate.

1

1 51. (Currently Amended) The article of manufacture of claim 43, wherein the
2 content, when accessed, further causes the ~~machine~~ computer to import the signed
3 certificate to a server associated with the identified certificate signing request.

1

1 52. (Currently Amended) The article of manufacture of claim 51, wherein the
2 content, when accessed, further causes the ~~machine~~ computer to import the signed
3 certificate to a device that performs SSL processing on behalf of the server.

1

1

1 53. (Currently Amended) The method of claim 43, wherein the content, when
2 accessed, further causes the ~~machine~~ computer to identify at least two certificate signing
3 requests associated with the signed certificate.

1

1 54. (Currently Amended) An article of manufacture comprising:
2 a ~~machine-accessible~~ computer readable medium providing content that, when accessed
3 by a ~~machine~~ computer, causes the ~~machine~~ computer to
4 generate a certificate signing request, the certificate signing request including
5 distinguished name data;
6 store the distinguished name data in a mapping table;
7 transmit the certificate signing request to a certificate authority;
8 receive a signed certificate from the certificate authority, the signed certificate
9 including distinguished name data;
10 extract the distinguished name data from the signed certificate; and
11 compare the extracted distinguished name data with the stored distinguished name
12 data contained in the mapping table to identify the certificate signing
13 request.

1

1 55. (Original) The article of manufacture of claim 54, the stored distinguished
2 name data comprising all of the distinguished name data contained in the certificate
3 signing request.

1

1

1 56. (Original) The article of manufacture of claim 54, the stored distinguished
2 name data comprising a common name.

1

1 57. (Currently Amended) The article of manufacture of claim 54, wherein the
2 content, when accessed, further causes the ~~machine~~ computer to compare a portion of the
3 extracted distinguished name data with a portion of the stored distinguished name data.

1

1 58. (Currently Amended) The article of manufacture of claim 54, wherein the
2 content, when accessed, further causes the ~~machine~~ computer to compare a common
3 name contained in the extracted distinguished name data with a common name contained
4 in the stored distinguished name data.

1

1 59. (Original) The article of manufacture of claim 54, the extracted
2 distinguished name data comprising all of the distinguished name data contained in the
3 signed certificate.

1

1 60. (Original) The article of manufacture of claim 54, the extracted
2 distinguished name data comprising a common name.

1

1

1 61. (Currently Amended) The article of manufacture of claim 54, wherein the
2 content, when accessed, further causes the ~~maehine~~ computer to:
3 generate a key pair associated with the certificate signing request; and
4 identify the key pair when comparing the extracted distinguished name data with the
5 stored distinguished name data.

1

1 62. (Currently Amended) The article of manufacture of claim 54, wherein the
2 content, when accessed, further causes the ~~maehine~~ computer to import the signed
3 certificate to a server associated with the certificate signing request.

1

1 63. (Currently Amended) The article of manufacture of claim 54, wherein the
2 content, when accessed, further causes the ~~maehine~~ computer to import the signed
3 certificate to an SSL processing device.